UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/761,173	01/16/2001	Russell Dellmo	GCSD-1131 (51211)	4910

27975 7590 05/26/2006

ALLEN, DYER, DOPPELT, MILBRATH & GILCHRIST P.A.
1401 CITRUS CENTER 255 SOUTH ORANGE AVENUE
P.O. BOX 3791
ORLANDO, FL 32802-3791

EXAMINER	
TRAN, TONGOC	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 05/26/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/761,173
Filing Date: January 16, 2001
Appellant(s): DELLMO ET AL.

Cian G. O'Brien
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed on March 17, 2006 appealing from the Office action mailed September 20, 2005.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The amendment after final rejection filed on November 21, 2005 has not been entered.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The summary of claimed subject matter contained in the brief is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

U.S. 6,480,477 B1	**Treadaway et al.**	**11-2002**
U.S. 2001/0021926 A1	**Schneck et al.**	**9-2001**
U.S. 6,259,933 B1	**Bambridge et al.**	**7-2001**
U.S. 2002/0114,288 A1	**Soliman**	**8-2002**

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 16, 8, 10, 13-18, 21, 24-28, 30-34, 36-41 and 43-50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Treadaway et al. (U.S. Patent No. 6,480,477, hereinafter Treadaway) in view of Schneck et al. (U.S. PGPUB 2001 /0021926A1, hereinafter Schneck) and Bambridge et al. (U.S. Patent No. 6,259,933, hereinafter Bambridge).

In respect to claim 1, Treadaway discloses a secure wireless local area network (LAN) device comprising: a wireless transceiver; a media access controller (MAC); and a cryptography circuit carried by said housing and connected to said MAC and said wireless transceiver (Treadaway, col. 3, lines 35-58 and col. 4, lines 8-11),

Treadaway does not disclose but Schneck discloses said cryptography circuit operating using cryptography information and rendering unusable the cryptography information based upon tampering (Schneck, [0067]). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teaching of Schneck's rendering cryptography information unusable upon tampering with Treadaway's teaching of including cryptographic apparatus in the MAC device in order to protect the cryptographic information from tampering.

Furthermore, Treadaway does not explicitly disclose but Bambridge discloses a MAC board is mounted within a housing (Bambridge, col. 5, lines 25 40). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teaching of Bambridge to include a housing unit with the teaching of Treadaway's MAC that including cryptographic apparatus and wireless transceiver in order to protect security protection.

In respect to claim 2, Treadaway, Schneck and Bambridge disclose the secure wireless LAN device according to Claim 1 wherein said cryptography circuit comprises:

at least one volatile memory for storing the cryptography information; and a battery for maintaining the cryptography information in said at least one volatile memory (Schneck, [0067]).

In respect to claim 3, Treadaway, Schneck and Bambridge disclose the secure wireless LAN device according to Claim 2 wherein said cryptography circuit further comprises at least one switch operatively connected to said housing for disconnecting said battery from said at least one volatile memory so that the cryptography information therein is lost based upon breach of said housing (Schneck, [0067]).

In respect to claim 4, Treadaway, Schneck and Bambridge disclose the secure wireless LAN device according to Claim 1 wherein said cryptographic information comprises a cryptography key (Treadaway, col. 23, lines 47-67).

In respect to claim 5, Treadaway, Schneck and Bambridge disclose secure wireless LAN device according to Claim 1 wherein said security information comprises at least a portion of a cryptography algorithm (Treadaway, col. 23, lines 47-67).

In respect to claim 6, Treadaway, Schneck and Bambridge disclose secure wireless LAN device according to Claim 1 wherein said MAC implements a predetermined wireless LAN MAC protocol (Treadaway, col. 6, lines 57-67).

In respect to claim 8, Treadaway, Schneck and Bambridge disclose the secure wireless LAN device according to Claim 1 further comprising at least one connector carried by said housing for connecting to at least one of a user station

and an access point (Treadaway, col. 3, lines 35-50 and col. 27, lines 28-40).

In respect to claim 10, Treadaway, Schneck and Bambridge disclose the secure wireless LAN device according to Claim 1 wherein said cryptography circuit comprises:

a cryptography processor; and a control and gateway circuit connecting said cryptography processor to said MAC and said wireless transceiver (Treadaway, col. 3, lines 35-58 and col. 23, lines 47-67).

In respect to claim 13, the claim limitation is substantially similar to claims 1 and 8. Therefore, claim 13 is rejected based on the similar rationale.

In respect to claims 14-18 and 21, the claim limitations are substantially similar to claims 2-6 and 10. Therefore, claims 14-18 and 21 are rejected based on the similar rationale.

In respect to claim 24, the claim limitation is substantially similar to claims 1 and 2. Therefore, claim 24 is rejected based on the similar rationale.

In respect to claims 25-28, the claim limitations are substantially similar to claims 3-7. Therefore, claims 25-28 are rejected based on the similar rationale.

In respect to claim 30, the claim limitation is substantially similar to claims 1, 2 and 8. Therefore, claim 30 is rejected based on the similar rationale.

In respect to claims 31-34, the claim limitations are substantially similar to claims 3-6. Therefore claims 31-34 are rejected based on the similar rationale.

In respect to claim 36, the claim limitation is substantially similar to claims 1 and 8. Therefore, claim 36 is rejected based on the similar rationale.

In respect to claims 37-41, and 43-44, the claim limitations are substantially similar to claims 2-6 and 8. Therefore, claims 37-41 and 43-44 are rejected based on the similar rationale.

In respect to claims 46-50, the claim limitations are method claims that are substantially similar to the system claims 1 and 3-6. Therefore, claims 46-50 are rejected based on the similar rationale.

2. Claims 7, 9, 19-20, 29, 35, 42 and 51 are rejected under 35 U.S.C. 103(a) as being unpatentable over Treadaway et al. (U.S. Patent No. 6,480,477, hereinafter Treadaway) in view of Schneck et al. (U.S. PGPUB 200110021926A1, hereinafter Schneck) and Bambridge et al. (U.S. Patent No. 6,259,933, hereinafter Bambridge) and further in view of Baldwin et al. (U.S. Patent No. 6,560,448, hereinafter Baldwin).

In respect to claim 7, Treadaway, Schneck and Bambridge disclose the secure wireless LAN device according to Claim 6 wherein said predetermined wireless LAN MAC protocol is based upon the IEEE 802.3u standard but not the IEEE 802.11 standard. However, Baldwin discloses implementing IEEE 802.11 for wireless LAN communication protocol. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to improve the teaching of Treadaway with the teaching of Baldwin new standard in order to adapt to the new changes in the wireless local area network.

In respect to claim 9, Treadaway, Schneck and Bambridge do not disclose but Baldwin discloses a secure wireless LAN device wherein said at least one connector comprises a PCMCIA connector (Baldwin, col. 7, lines 12-41). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the teaching of PCMCIA connector taught by Baldwin with the teaching of secure wireless LAN taught by Treadaway for the benefit of implementing PCMCIA card that can be plugged in on a PC card slot.

In respect to claims 19-20, 29, 35, 42 and 51, the claim limitations are substantially similar to claims 7 and 9. Therefore, claims 19-20, 29, 35, 42 and 51 are rejected based on the similar rationale.

3. Claims 11 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Treadaway et al. (U.S. Patent No. 6,480,477, hereinafter Treadaway) in view of Schneck et al. (U.S, PGPUB 2001/0021926A1, hereinafter Schneck) and Bambridge et al. (U.S. Patent No. 6,259,933, hereinafter Bambridge) and further in view of Soliman (U.S. PGPUB 2002/0114288).

In respect to claim 11, Treadaway, Schneck and Bambridge do not disclose but Soliman discloses the secure wireless LAN device according to Claim 1 wherein said wireless transceiver comprises:

a baseband processor;

a modem connected to said baseband processor; and a radio frequency transmitter and receiver connected to said modem ([0076]). It would have been obvious

to one of ordinary skill in the art at the time the invention was made to incorporate the different components of wireless transceiver taught by Soliman with Treadaway's wireless transceiver for these components are common found in typical wireless transceiver unit.

In respect to claim 22, the claim limitation is substantially similar to claim 11. Therefore, claim 22 is rejected based on the same rationale.

4. Claims 12 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Treadaway et al. (U.S. Patent No. 6,480,477, hereinafter Treadaway) in view of Schneck et al. (U.S. PGPUB 2001/0021926A1, hereinafter Schneck) and Bambridge et al. (U.S. Patent No. 6,259,933, hereinafter Bambridge) and further in view of Treadaway et al. (U.S. Patent No. 6,665,285, hereinafter Treadaway ['285]).

In respect to claim 12, Treadaway, Schneck and Bambridge do not disclose but Treadaway ['285] discloses at least one antenna carried by said housing and connected to said wireless transceiver (Treadaway ['285]). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the components in the wireless LAN teaching of Treadaway ['285] with the teaching of Treadaway's secure wireless LAN for the broadcasting purposes.

In respect to claim 23, the claim limitation is substantially similar to claim 12. Therefore, claim 23 is rejected based on the similar rationale.

(10) Response to Argument

Claim 1 and 24:

In response to Appellants' argument to rejected claim 1. Appellants contend that the cited prior art Treadaway et al. do not provide proper suggestion or motivation to combine the feature of tamper detection taught by Schneck et al. because the prior art devices are not physically combinable. However, the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference. Rather the test is what the combined teachings of those references would have suggested to those of ordinary skill in the art" In re Keller, 642 F.2d 413, 425, 208 USPQQ 871, 881 (CCPA 1981). See also In re Sneed, 710 F.2d 1544, 1550, 218 USPQ 385, 389 (Fed. Cir. 1983) ("[I]t is not necessary that the invention of the references be physically combinable to render obvious the invention under review."); and In re Nievelt, 482 F.2d 965, 179 USPQ 224, 226 (CCPA 1973) ("Combining the teachings of references does not involved an ability to combine their specific structures."). Examiner asserts that the combination of the prior art teachings does not changed the principle of the operation of the primary references taught by Treadaway et al. or render the reference inoperable for its intended purpose. The second reference, Schneck et al., is merely used to echo the well known teaching that volatile memory can not retain data once the power is removed. Schneck et al. also address the well known concern that stored secret such as cryptographic data is subject

to physical tampering and in order for cryptographic data to be protected, there is a need to enable this information to be self-destroyed upon tampering (Schneck, [0067]). Treadaway et al. teach the incoming and outgoing Ethernet data packets are passing through an encryption decryption processing unit as illustrated in Fig. 16. The fact that security of stored secret is always a concern; Therefore, taking measure to protect secure information such as *stored cryptographic information (e.g. algorithms or keys)* that is subject to tampering would have been obvious. One of ordinary skill in the art would have been motivated to adapt the teaching of storing the cryptographic information taught by Treadaway with the teaching of Schneck et al. by providing a mechanism to ensure the information is self destroyed by removing the power of the volatile memory used to maintained stored secret data.

In response to Appellants' argument that claim 24 is rejected based on the same rationale of the rejected claim 1 and the Examiner has failed to address the cited limitation of "at least one volatile memory 107 for storing the cryptography information, and a battery 109 for maintaining the cryptography information in the at least one volatile memory". Examiner rejected claim 24 based on the similar rationale as rejected claim 1 because the cited portion of prior art, Schneck et al., has been cited in claim 1 to teach the advantage of storing secure data in a volatile memory since data can not be retained once the power (or battery) is removed (Schneck, [0067], Office Action page 3).

Claims 13 and 30:

In response to Appellants' argument that claims13 and 30 are rejected based on the same rationale of the rejected claim 1 and therefore the cited limitation of "at least one connector carried by said housing for connecting to at least one of a LAN station and a LAN access point" has not been addressed. Treadaway teach the wireless link is coupled to the LAN (e.g. Fig. 3, item *108 (Connector)*, 106 (100BASE-T, Ethernet standard and 212 (transceiver); Fig. 4, item 222 (MAC); and col. 7, lines 1-9). These claims and claim 1 recite the secure wireless *local area network (LAN) device* comprises *a media access controller* (MAC) which is the part of the OSI network model data link layer that determines who is allowed to access the physical media at any one time. It acts as an interface between the Logical Link Control sublayer and the network's physical layer. Since it acts as *an interface* between the Logical Link and the network's *physical layer*, at least a connector connecting to a LAN station would have been obviously encompassed in the claimed device that comprise the MAC unit recited in claim 1 in order for the device to worked in the LAN environment as recited in the preamble.

Claims 36 and 46:

In response to Appellant's argument to claims 36 and 46, the claimed limitations are system and method claims claiming the similar limitations as claim 1. Appellants contend that the cited prior art Treadaway et al and Schneck et al. do not provide suggestion or motivation to combine. Examiner asserts that the teaching of Schneck et

al. is merely to echo the well known teaching that volatile memory can not retain data once the power is removed. Schneck et al. also address the well known concern that stored secret such as cryptographic data is subject to physical tampering and in order for cryptographic data to be protected, there is a need to enable this information to be self-destroyed upon tampering. One of ordinary skill in the art would have been motivated to adapt the teaching of storing the cryptographic information taught by Treadaway with the teaching of Schneck et al. by providing a mechanism to ensure the information is self destroyed by removing the power of the volatile memory used to maintained stored secret data.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Examiner: Tongoc Tran

Art Unit: 2134

Conferees:

Jacques Louis-Jacques JLJ

SPE, Art Unit: 2134

Gilberto Barron JR

SPE, Art Unit: 2132

JACQUES H. LOUIS-JACQUES
PRIMARY EXAMINER